

GENERAL RECORDS SCHEDULE XXX

Information Technology Operations and Management Records

DRAFT

May 24, 2000

This schedule provides disposal authorization for files that are created and maintained for the operation and management of information technology (IT) and related services. As defined in the Information Technology Management Reform Act of 1996, "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. This schedule covers only records relating to overall management and operation of the agency's information technology infrastructure including network systems and applications. It does not provide disposal authority for any records relating to specific systems or applications that support program activities of the agency. In particular, items 13-15 do not cover records relating to development, implementation, operation, management, and modification of systems and applications that support one or more program offices or functions.

This GRS does not apply to the records of agencies under the Executive Office of the President.

This GRS does not cover all records that are used in IT operations and management.

- IT offices maintain many common administrative files covered by other GRS, e.g., personnel, accounting, and travel records. The other GRS apply to those records in IT offices as well as elsewhere.
- IT offices may maintain other files whose disposition is authorized under records schedules applicable to the entire agency or component in which the IT office is located. IT offices should apply such schedules, as appropriate.
- IT offices may maintain unique files, such as IT strategic plans and Business Information Models, that are related to IT operations and management. Such files must be covered by a schedule approved by NARA.

The disposition instructions in this schedule apply only to records that are maintained as described in each item or subitem. If documents are part of a larger subject or case file, you must use the disposition instructions for the subject or case file.

This schedule applies to the records described regardless of their physical form or characteristics. They may be retained on paper, in microform, or in electronic form.

PROCEDURES

1. Implementation and oversight files.

Records in offices with agency-wide or bureau-wide responsibility for managing IT operations relating to implementation and compliance with IT policies, directives and plans including recurring and special reports, responses to findings and recommendations, and reports of follow-up activities.

a. Performance measurements and benchmarks.

Destroy/delete 1 year after determination that there are no unresolved issues.

b. Other records including

- audits and management reviews
- certifications and accreditation
- quality assurance reviews and reports
- reports on implementation of plans
- effectiveness evaluations, and compliance reviews
- data measuring or estimating impact and compliance

Destroy/delete 3 years after determination that there are no unresolved issues.

[NOTE: See item 3 for performance files relating to systems.]

2. IT facility and site management and equipment support files.

Records maintained by offices responsible for IT programs that document the control and operation of buildings and rooms where IT equipment, systems, and storage media are located, including files identifying IT facilities and sites, and files concerning implementation of IT facility and site management and equipment support services provided to specific sites, including reviews, site visit reports, trouble reports, equipment service histories, reports of follow-up actions, and related correspondence.

Destroy/delete when 3 years old.

3. IT asset and configuration management files.

a. Records identifying or inventorying IT assets; equipment control systems; inventories of network circuits and building or circuitry diagrams.

Place record in inactive file when the subject assets are terminated, removed or destroyed. Cut off inactive file annually. Destroy/delete 1 year after close of file.

b. Records created and retained for asset management, performance and capacity management, system management, configuration and change management, and planning, follow-up and impact assessment of specific systems. Includes, but is not limited to:

- (1) Data and detailed reports on implementation of systems, applications and modifications; assessments of effectiveness, application sizing, resource and demand management; documents identifying, requesting, and analyzing possible changes, authorizing changes, and documenting implementation of changes; documentation of software distribution and release management.

Retain for life of system. Destroy 1 year after termination of system.

- (2) Records of IT maintenance on the network infrastructure documenting preventative, corrective, adaptive and perfective (enhancement) maintenance actions, including requests for service, work orders, service histories, and related records.

Close file annually. Destroy/delete 3 years after close of file.

4. Tape Library Records.

- a. Automated files used to control the location, maintenance, and disposition of magnetic media in a tape library.

Destroy after related records or media are destroyed or withdrawn from the tape library.

- b. Records used to control the location, maintenance, and disposition of magnetic media in a tape library including list of holdings and control logs.

Destroy when superseded.

- c. System backup tapes.

- (1) Destroy incremental backup tapes when superseded by a full backup.
- (2) Destroy full backup tapes when second subsequent backup is verified as successful.

SECURITY OF SYSTEMS AND DATA

5. Files related to maintaining the security of systems and data.

Documents identifying IT risks and analyzing their impact, risk measurements and assessments, actions to mitigate risks, implementation of risk action plan, service test plans, test files and data.

Close file annually. Destroy/delete 3 years after system superseded.

6. User identification, profiles, authorizations, and password files.

EXCLUDES records relating to electronic signatures.

Place record in inactive file when user account is terminated or when profile or password is altered. Cut off inactive file quarterly. Destroy/delete inactive file 6 months after cutoff.

7. Security incident handling, reporting and follow-up.

Close file when all necessary follow-up to a security incident has been completed.
Destroy/delete 3 years after close of file.

8. Files on usage and monitoring of IT systems, services, and resources.

a. Usage and monitoring data and reports, including but not limited to:

Operations data, such as system event logging, log-in files, system usage files and audit trails, reports on workload management; incident reports and audit trails of problems and solutions, usually in electronic format.

Destroy/Delete 90 days after creation.

b. Reports on operations, including summary computer usage reports, measures of benchmarks, performance indicators, and critical success factors; error and exception reporting, self-assessments, service delivery monitoring, and management reports.

Close files annually. Destroy/delete 3 years after close of file.

OPERATIONS AND SERVICES

9. IT operations records.

a. Schedules: workload schedules; run reports, run requests, and other records documenting the successful completion of a run; schedules of maintenance and support activities.

Close file annually. Destroy/delete 1 year after close of file.

b. Problem reports, user complaints and questions, proposals for changes and related decision documents relating to the software infrastructure of the network or system.

Destroy/delete when 3 years old.

10. Financial records related to provision of IT resources and services.

a. Service-level agreements formalizing performance criteria for quantity and quality of service, including definition of responsibilities, response times and volumes, charging, integrity guarantees, non-disclosure agreements.

Close file when the agreement is superseded or terminated. Destroy/delete 3 years after close of file.

b. Files related to managing third-party services: control measures for review and monitoring of contracts, procedures for determining their effectiveness and compliance.

Close file when subject control measures or procedures are superseded or terminated.
Destroy/delete 3 years after close of file.

- d. Records generated in IT management and service operations to identify and allocate charges and track payments for computer usage, data processing and other IT services EXCLUDING records that are part of the agency's cost accounting system, which are covered in GRS 8, items 6 and 7.

Close file annually unless there are outstanding issues concerning charges or payments. If there are outstanding issues, close file when they are resolved. Destroy/delete 3 years after close of file.

[NOTE: Copies of records needed to support contracts should be filed in procurement files which are scheduled under GRS 3.]

11. Records Relating to IT Management and Reporting Required by ITMRA.

- a. Strategic plan documenting how information resources will support agency missions, goals, and objectives, related background records, and records relating to the development and implementation of performance measures and procedures.

Close file when plan is superseded or terminated. Destroy 5 years after close of file.

- b. Annual report to Congress and related developmental and background records.

Destroy when 5 years old.

- c. Information technology resources inventory of major systems and initiatives and related developmental and background records.

Close file when superseded. Destroy 5 years after close of file.

12. Customer service files.

Records related to providing service and individual support to customers, including pamphlets, responses to "Frequently Asked Questions," and other documents prepared in advance to assist customers; help desk logs and reports and other files related to customer query and problem response; query monitoring and clearance; and customer feedback records; and related trend analysis and reporting.

Place in inactive file when action is completed or guidance is superseded or obsolete. Close file annually. Destroy/delete 1 year after close of file.

PROJECT MANAGEMENT

13. IT Project Case Files.

Records of IT projects undertaken to support specific IT infrastructure and network initiatives in accordance to the long term operational, technological, infrastructure and data processing service planning activities of the IT shop. Includes records used to define and

track requirements for IT resources - such as hardware, software, and services – which support more than one operation, such as network-wide software implementations and upgrades for personal computers; files relating to the installation and acceptance/accreditation of systems and components that support multiple network applications, including plans and reports concerning the evaluation of options, feasibility, costs and benefits, as well as the installation, migration, conversion, and acceptance of hardware, software, netware, and related models, diagrams, schematics, and related data and technical documentation.

[NOTE: Items 13a and 13b do not apply to project records relating to specific systems that support or document mission goals.]

a. Project Case Files where the final decision is not to implement recommendations.

Close file when final decision on recommendations is made. Destroy/delete 1 year after close of file.

b. Project Case Files where one or more recommendations for satisfying IT requirements are implemented.

Close file when it is determined that the requirement no longer exists or that a new requirements analysis should be undertaken. Destroy/delete 5 years after close of file.

14. Files related to infrastructure and network system implementation and modification.

Records relating to implementation and modification of systems that are part of the agency's information technology infrastructure and agency networks, including software and upgrades for desktop applications for networked personal computers.

Includes:

- data and detailed reports on implementation and modification of IT infrastructure and network systems
- assessments of effectiveness, application sizing, resource and demand management
- documents identifying, requesting, and analyzing possible changes, authorizing changes, and documenting implementation of changes
- listings of potential problems, test plans, test data, test procedures and results, final validation results
- quality assurance reviews
- documentation of software distribution and release management
- records relating to computer century conversion ("Y2K") activities

[NOTE: This item does not apply to project records relating to specific systems that support or document mission goals.]

Close file annually. Destroy/delete 3 years after close of file.

15. Files relating to application development and implementation.

[NOTE: Items 15a and 15b do not apply to project records relating to specific systems that support or document mission goals.]

- a. Application development case files. Records created and used in determining customer needs for applications, designing, developing, acquiring, or modifying applications including user requirements and specifications, system or subsystem specifications, system integration documents, application and data deployment strategies, status reports, records documenting acceptance of applications and modifications, and related correspondence.

Close file when application is no longer needed or when all records supported by the application are destroyed, or when records have been migrated to a new platform.

Destroy/delete 3 years after close of file.

- b. Installation and testing records for applications.

Close file when final decision on acceptance is made. Destroy/delete 3 years after close of file.